☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with Apple ID moneysigns1000@gmail.com that is stored at premises controlled by Apple Inc.

Case No. 24-M-416 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 5-30-24 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 5-16-24. 10:00 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

Stephen C. Dries, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID **moneysigns1000@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from January 1, 2023 through December 12, 2023, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 21 U.S.C. §§ 841(a)(1), 846, 856(a) and 18 U.S.C. §§ 922(g)(1) and 924(c), those violations involving Montreal KELLY since January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The sale of illegal drugs, the laundering of proceeds of drug sales, and the illegal possession of firearms;

(b) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and the account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s); and

(e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Apple ID moneysigns1000@gmail.com that is stored at premises controlled by Apple Inc.

Case No. 24-M-416 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC. §§ 841(a)(1), 846, & 856(a); 18 USC §§ 922(g)(1) & 924(c)	Possession with intent to distribute & conspiracy to distribute controlled substances; maintaining drug premises; illegal possession of firearms

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DEA TFO Robert Gregory
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 5-16-24

Judge's signature

City and state: Milwaukee, Wisconsin

Stephen C. Dries, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Robert Gregory, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Agency, and I am a certified State of Wisconsin Law Enforcement Officer since 2013 and a Police Officer with the Milwaukee Police Department. I am currently assigned to North Central High Intensity Drug Trafficking Area Interdiction Unit which is involved in the investigation of offenses involving but not limited to narcotics, narcotics trafficking and individuals prohibited from possessing firearms. I am an investigator or law enforcement officer of

the United States within the meaning of US U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal felony arrests.

3. As a Police Officer and a Task Force Officer, I have participated in the investigation of numerous narcotics-related offenses, resulting in the prosecution and conviction of individuals and the seizure of illegal drugs, weapons, United States currency and other evidence of criminal activity. As a narcotics investigator, I have interviewed many individuals involved in drug trafficking and have obtained information from them regarding the acquisition, sale, importation, manufacture, and distribution of controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology used by the traffickers and abusers of controlled substances. I have participated in all aspects of drug investigations, including physical surveillance, execution of search warrants, undercover operations, analysis of phones and the arrests of numerous drug traffickers. I have also been the affiant of many search warrants.

4. Additionally, I have spoken with other experienced narcotics investigators on numerous occasions concerning the method and practices of drug traffickers and money launderers. Furthermore, I have attended training courses that specialized in the investigation of narcotics trafficking and money laundering. Through these investigations, my training and experience, and conversations with other law enforcement personnel, I have become aware with the methods used by drug traffickers

to manufacture, smuggle, safeguard, and distribute narcotics, and to collect and launder trafficking-derived proceeds. I am further aware of the methods employed by major narcotics organizations to thwart any investigation of their illegal activities.

5. Based on my training and experience, I know that criminal investigations have been aided by subpoenas, warrants, and court orders by providing critical investigative leads and corroborative evidence.

6. Based on my training, experience, and participation in drug trafficking investigations and associated financial investigations involving controlled substances, I know and have observed the following:

a. I know large-scale drug traffickers often purchase and/or title their assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own, use and exercise dominion and control over these assets;

b. I know large-scale drug traffickers must maintain on-hand, large amounts of U.S. currency to maintain and finance their ongoing drug business;

c. Drug traffickers frequently possess firearms and ammunition to protect their illegal product;

d. I know that drug traffickers engaged in mobile drug trafficking often use their vehicles to facilitate their trafficking activities by transporting and/or securing contraband including but not limited to controlled substances, packaging materials and other tools of the drug trade, drug proceeds, and firearms;

e. I know it is common for persons involved in large-scale drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, passbooks, letters of credit, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses, vehicles, or other locations over which they maintain dominion and control;

f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned book,

records, receipts, notes, ledger, etc., are maintained where the traffickers have ready access to them;

g. It is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses, offices, personal residence, or device storage.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. To this end, based upon my training and experience, I know that individuals involved in drug trafficking frequently use cellular telephones to maintain contact and arrange transactions with their sources and customers of and co-conspirators in the distribution of controlled substances. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in "text" format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs. I also believe that it is common for crime suspects who possess illegal controlled substances and firearms to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and firearms that they control, possess, buy, and sell

9. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) (distribution of and possession with intent to distribute controlled substances), 846 (drug conspiracy), 856(a) (maintaining a drug-involved premises); 18 U.S.C. § 922(g)(1) (felon in possession of a firearm); and 18 U.S.C. § 924(c) (possession of a firearm in furtherance of a drug trafficking crime) have been committed by Montreal KELLY. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

11. On December 12, 2023, law enforcement officers executed a federal search warrant at 4503 N. 57th Street, Milwaukee, Wisconsin, the residence of Montreal KELLY. Upon entering the residence, KELLY was observed coming up from the basement. Officers also encountered KELLY's girlfriend, Fredricka Rivera, and three young children in the residence.

12. Upon searching, officers observed water on the toilet seat and on the floor of the bathroom, along with a razor blade wrapped in what appeared to be a towel, and

stray U.S. currency strewn about the bathroom floor. In the kitchen, law enforcement officers located and seized a black digital scale and a kitchen knife covered in white residue on the kitchen counter. The scale and knife were located on top of a dumbbell weight, which officers believe based on their training and experience can be used as makeshift drug press. Officers also located numerous open sandwich boxes and loose unused and used clear plastic sandwich bags on the kitchen counter and in a kitchen drawer. In the kitchen cabinet above the microwave, officers located a clear plastic bag containing a white powder substance, a Pyrex measuring cup with white residue, and baking soda. Officers also seized a loaded, silver-over-black, Smith and Wesson 9mm semi-automatic handgun, bearing Serial Number FBB3648, which was lying on the kitchen counter. KELLY's wallet was on the kitchen counter directly next to the firearm. Officers also located a small amount of marijuana and some loose ammunition from a kitchen drawer. In the basement, officers located three blenders with white powder residue and another Pyrex measuring cup with white residue. Additionally, officers located digital scales in two of the vehicles and a small amount of white powder in a plastic bag in one of the vehicles. Based on their training and experience, case agents believe that the evidence located in KELLY's residence is consistent with him using the residence to manufacture controlled substances.

13. Officers subjected the seized white powder residue, totaling just over 1 gram, to laboratory testing, which came back as containing no controlled substances.

14. On the morning of December 12, 2023, KELLY stated that the firearm

located in his house belonged to his girlfriend, Rivera. Rivera was questioned about the firearm, and she stated that the firearm was hers, that she purchased it, and that she knew KELLY had possession of it the previous few days. Rivera stated that KELLY would go into the basement and use the blender to mix controlled substances in the residence. Rivera further stated that when officers began knocking on the door, KELLY was in the bathroom, ran downstairs, and then ran back to the bathroom. Based on their training and experience, as well as the evidence gathered during the course of the investigation, case agents believe that KELLY flushed controlled substances down the toilet before law enforcement officers entered the premises.

15. KELLY was arrested on December 12, 2023. Upon his arrest, located in KELLY's front left pants pocket was a black Apple iPhone with damage to the back. KELLY was not willing to provide case agents with the passcode to his phone.

16. On December 14, 2023, the Honorable Stephen C. Dries, United States Magistrate Judge, authorized a search warrant for KELLY's black Apple iPhone. A forensic examination was thereafter performed, however the phone was not able to be fully extracted. Rather, agents only obtained a partial extraction.

17. KELLY's black Apple iPhone was associated with Apple ID **moneysigns1000@gmail.com**. The phone number associated with the phone was (414) 243-8555.

18. The partial extraction reflected the following:

a. On February 17, 2023, a picture contained within the Notes reflected a series of numbers that case agents believe to be in reflective of how

many bill denominations were contained within a stack of money, for a total amount of $33,980. *See* Figure 1. Case agents know based on their training and experience that drug trafficking is a cash business and that traffickers often use money counters to tally drug proceeds, which are used as payment for controlled substances. Case agents believe the note is a tally of drug proceeds earned through trafficking or paid to a supplier.

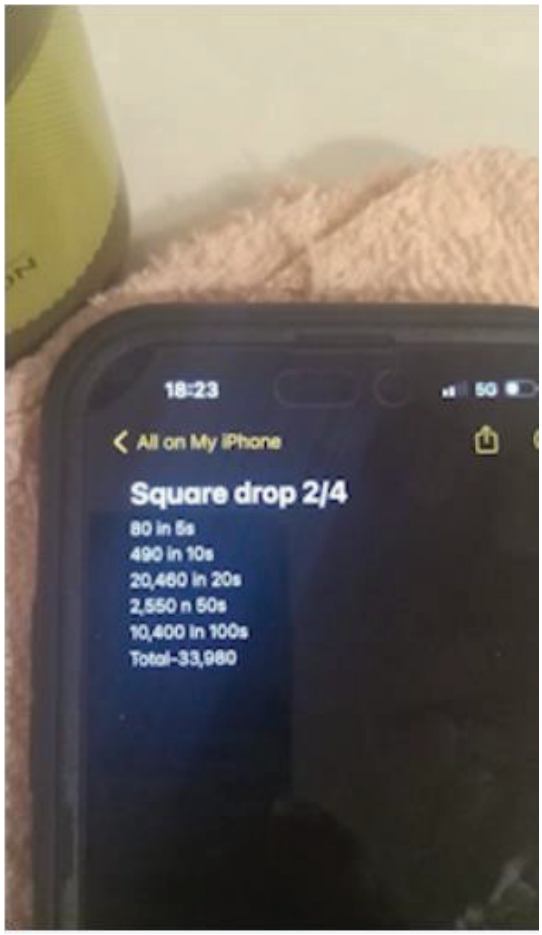

Figure 1

b. A photograph dated June 10, 2023, depicting two black rifles with the barrel pointed towards the ground and leaning against a person's leg and with a hand on the handle of one of the rifles. *See* Figure 2.

Figure 2

c. A photograph dated May 13, 2023, depicting the image of a cellphone displaying the message, "Got 250 for HP." Based on their training and experience, case agents believe "HP" is a reference to a "half pound" of a controlled substance, likely marijuana, and that "250" is the price the half pound costs. *See* Figure 3.

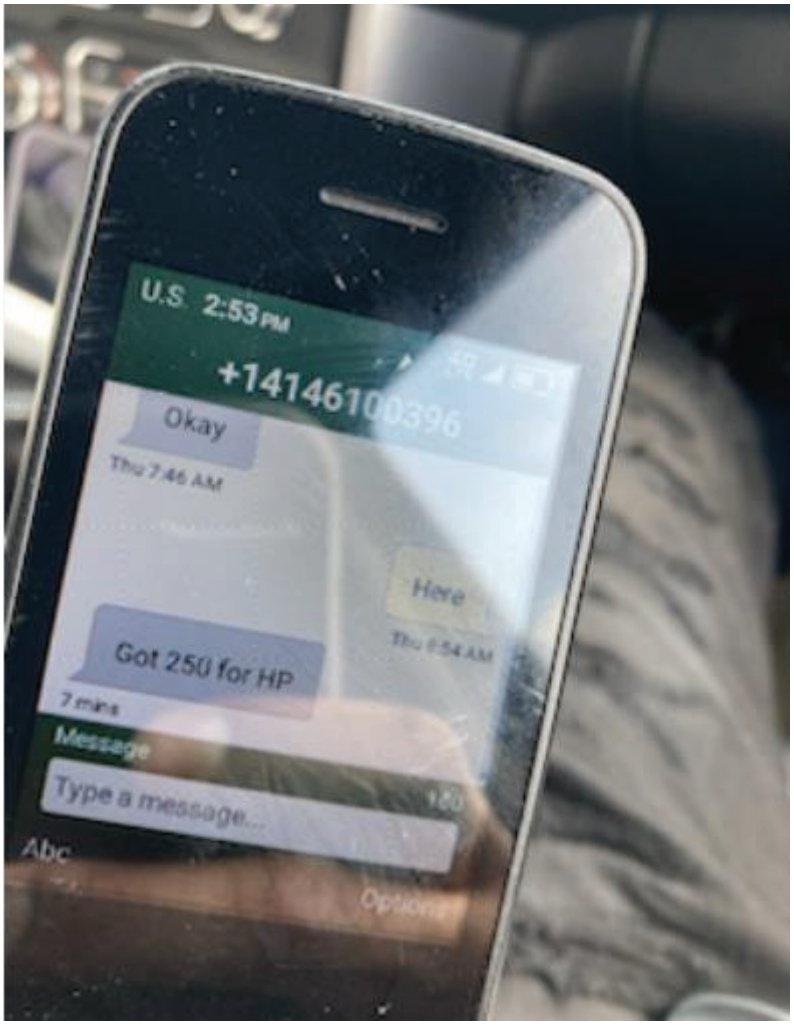

Figure 3

d. A photograph dated October 7, 2023, believed to depict a silver and black Smith and Wesson handgun, which is consistent with the firearm that was seized during the warrant execution as detailed above. *See* Figure 4.

Figure 4

e. A photograph dated March 19, 2023, depicting a male standing at a counter with U.S. currency stacked the width of the island and a black handgun near the money. The photograph appears to have been taken inside KELLY's residence at his kitchen island. *See* Figure 5. Case agents believed based on their training and experience that drug traffickers take photographs of themselves with large amounts of U.S. currency because it is a cash business and can be very lucrative. Furthermore, case agents know that drug traffickers often possess firearms to protect their illegal product and their drug proceeds.

Figure 5

19. A check of Wisconsin Circuit Court Access revealed KELLY was convicted of two counts of Burglary-Building or Dwelling, in violation of Wisconsin State Statute 941.10(1m)(a) in Milwaukee County Case No. 2011CF007115, which is a felony offense. KELLY is therefore prohibited from possessing firearms.

20. KELLY has since been charged by indictment with controlled substance and firearms offenses, in violation of 21 U.S.C. § 856(a)(1) and 18 U.S.C. §§ 922(g)(1), 924(a)(8), and 924(c)(1)(A)(i). *See United States v. Montreal Kelly*, Case No. 23-M-517.

21. On November 1, 2023, case agents conducted a debrief with CHS #1 during which CHS #1 spoke about a person known to CHS #1 as "Blood." Case agents were aware of a person with the nickname "Blood" that was involved in the distribution of cocaine and heroin in southeastern Wisconsin who they identified as KELLY. Case agents showed CHS #1 a Milwaukee Police Department booking photograph of KELLY, and CHS #1 identified KELLY as the individual CHS #1's knows as "Blood."

22. CHS #1 informed case agents that CHS #1 has known KELLY since approximately 2014; however, CHS #1 re-connected with him around September 2021. CHS #1 stated that during the time CHS #1 and KELLY re-connected, KELLY informed CHS #1 that he (KELLY) was involved in the distribution of cocaine and offered to provide cocaine to CHS #1. KELLY brought CHS #1 to his (KELLY's) residence, and CHS #1 described the residence's location to case agents as being a single-family residence on the corner of N. 57th Street and W. Ruby Avenue. Case agents were aware that KELLY's residence is 4503 N. 57th Street, Milwaukee, Wisconsin, which was at the location CHS #1

described. CHS #1 stated during this first interaction at KELLY's residence, CHS #1 observed approximately 30 pounds of marijuana in tall blue tinted clear bags, approximately 2 or 3 kilogram-packages of cocaine, and approximately 2 kilogram-packages of fentanyl.

23. According to CHS #1, as a result of the quantity of cocaine and heroin that KELLY was in possession of and would continue to be in possession of, CHS #1 began a drug trafficking relationship with KELLY. CHS #1 stated over the next couple of months following September 2021, CHS #1 entered KELLY's residence multiple times a day to pick up between one and four ounces of cocaine from KELLY. CHS #1 stated KELLY would front the cocaine and CHS #1 would come back and pay KELLY around $850 per ounce for the cocaine that CHS #1 picked up. CHS #1 stated that in addition to the cocaine, KELLY fronted approximately 200 grams of pure fentanyl every week to CHS #1. CHS #1 stated that over time KELLY began to require CHS #1 to pick up more than one to four ounces of cocaine at a time to reduce the activity and frequency of visits at his residence in an attempt to avoid law enforcement detection. CHS #1 stated this drug trafficking relationship with KELLY lasted between approximately Fall 2021 and Spring 2023.

24. CHS #1 further stated that on at least eight occasions between the beginning of 2022 and spring of 2023, CHS #1 obtained at least one kilogram of cocaine from KELLY with an initial price of $29,000, which gradually dropped to $24,000. CHS #1 stated the most fentanyl that KELLY provided was 800 grams at one time. CHS #1 described the

cocaine as a white powder substance and was sold to CHS #1 in a pure, uncut form. CHS #1 stated that KELLY also sold the fentanyl to CHS #1 in a pure form and that the fentanyl was either white or had a purple tint.

25. CHS #1 stated KELLY was always in possession of multiple firearms inside of his residence, and the firearms would always be different. CHS #1 recalled observing multiple different handguns and multiple different AR style rifles inside his residence and stated that KELLY is a firearm enthusiast. CHS #1 described one occasion in which CHS #1 observed approximately $200,000 on a table inside KELLY's residence.

26. An analysis of phone records for a phone number used by CHS #1 between May 2022 and October 2022 reflects that CHS #1 communicated with a phone number that law enforcement officers believed to be used by KELLY.

27. Beginning in June 2023, CHS #1 made statements against CHS #1's penal interest. Thus far, the information provided by CHS #1 has been corroborated by information known to case agents gathered during the course of this investigation, including through independent investigation, various public databases, physical surveillance, and electronic surveillance. According to law enforcement databases, CHS #1 has a criminal history that includes felony drug convictions, misdemeanor convictions including resisting or obstructing, and other drug and fraud offenses resulting in fines. CHS #1 is cooperating for consideration on pending federal drug trafficking charges. Within the context of the information detailed and relied upon for purposes of this affidavit, case agents believe CHS #1 is credible and CHS #1's information reliable.

28. Based on the above, case agents believe that because KELLY used his iPhone tied to the Apple ID account, **moneysigns1000@gmail.com**, and the messages, notes, and photographs are incriminating in nature, there is reason to believe that there are additional messages, notes, contacts, and photographs saved in the iCloud account that will also be incriminating in nature.

29. On May 15, 2024, a preservation letter for Apple ID **moneysigns1000@gmail.com** was sent to Apple.

BACKGROUND CONCERNING APPLE[1]

30. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

31. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website

username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

32. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as

Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

33. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

34. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on

Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

35. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

36. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected

services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

37. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

38. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, notes, emails, voicemails, photos, videos, and

documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

39. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

40. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

41. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

42. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

43. Based on the forgoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID **moneysigns1000@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from January 1, 2023 through December 12, 2023, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 21 U.S.C. §§ 841(a)(1), 846, 856(a) and 18 U.S.C. §§ 922(g)(1) and 924(c), those violations involving Montreal KELLY since January 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The sale of illegal drugs, the laundering of proceeds of drug sales, and the illegal possession of firearms;

(b) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and the account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s); and

(e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature